ELSEVIER

Discrete Mathematics 213 (2000) 283–290

DISCRETE MATHEMATICS

Perfect binary codes: bounds and properties

F.I. Solov'eva

Sobolev Institute of Mathematics of the Siberian Division of Russian Academy of Sciences, pr. Koptyuga 4, 630090 Novosibirsk, Russia

Received 16 December 1996; revised 12 December 1997; accepted 14 February 1998

Abstract

Some nontrivial properties of perfect binary codes are discussed. We consider some constructions of perfect binary codes with the purpose to outline bounds on the number of nonequivalent perfect binary codes and we present the best known lower and upper bounds on the number of different perfect binary codes.

1. Introduction

The paper is devoted to single-error-correcting perfect binary codes (also called close-packed codes); we briefly call them perfect codes. The problems of the construction and enumeration of perfect codes are significant and complicated. We do not know now neither the classification of perfect binary codes nor a satisfactory nontrivial upper bound on the number of nonequivalent perfect codes.

We consider some properties and some constructions of perfect codes with the purpose to discuss the bounds on the number of nonequivalent perfect codes. The best known lower and upper bounds on the number of perfect codes of the given length are presented. We also consider some nontrivial properties of perfect binary codes such as the existence of nonsystematic perfect codes, the existence of kernels of all possible sizes for nonlinear perfect codes, etc. Some unsolved problems will be discussed.

2. Necessary definitions

A *binary code* C of length n is a subset (not necessarily subspace) of the n-cube E^n (the vector space of dimension n over GF(2)). The elements of C are called codewords or vectors. *The Hamming distance* between two vectors $x, y \in C$, denoted by $d(x, y)$,

☆ This research was supported by the Russian Foundation for Basic Research under grant 97-01-01104.

E-mail address: sol@math.nsc.ru (F.I. Solov'eva)

0012-365X/00/$ - see front matter
PII: S0012-365X(99)00188-0

is the number of coordinates in which the two vectors differ. *The Hamming weight* of the vector x is given by

$$\mathrm{wt}(x) = d(x, \theta),$$

where θ denotes the all-zero word. A code distance is given by $d = \min d(x, y) = \min \mathrm{wt}(x - y)$ for any different vectors $x, y \in C$. Two codes $C, C' \subset E^n$ are said to be *isomorphic* if there exists a permutation π of coordinates which maps the vectors of C into C'. Two codes $C, C' \subset E^n$ are *equivalent* if they are isomorphic or if the code C' is isomorphic to a translation of C, e.g. $C' = \{\pi(a) \oplus b\colon a \in C\}$, where π is the permutation and $b \in E^n$ is a fixed vector.

The union of spheres $K_t\{c\} = \{x \in E^n\colon d(c,x) \leqslant t\}$ of radius t with the centres c in the vectors of the set $M \subset E^n$ is called the *hull* of the set M and we denote this hull by $K_t(M)$. A set $C \subseteq E^n$ is called a perfect code of length n with code distance $d = 2t + 1$ if $K_t(C) = E^n$ and if $K_t\{v\} \cap K_t\{u\} = \emptyset$ for all $v, u \in C$.

In [30–32,26] it is shown that nontrivial perfect binary codes exist only in the following two cases:

(1) $d = 3$ and $n = 2^k - 1$, $k > 1$;
(2) $d = 7$ and $n = 23$.

The well-known binary Golay code is a perfect code of length $n = 23$; up to equivalence this code is uniquely determined. If $d = 3$ and $n = 2^k - 1$ many constructions of perfect codes exist. We give a list of these constructions and describe some of them with the goal to develop bounds on the number of perfect codes. From now on we consider only the case $d = 3$.

3. Short summary of constructions

The well-known Hamming codes are the only linear perfect codes (linear subspaces of the space E^n). In 1962, Vasil'ev [27] constructed a large number of nonequivalent perfect codes. In 1977, Heden [9] constructed perfect codes which are not equivalent to the Vasil'ev codes. The class of perfect codes described by Solov'eva in [21] (they are not equivalent to the Vasil'ev codes) contains the Heden codes properly. Two years later, Phelps [15] independently discovered Solov'eva's construction and generalized it [16]. Heden's construction properly contains the class of Laborde's codes [12], cf. [10]. A generalization of Vasil'ev's construction can be found in [14]. In 1970 and 1988, Zinov'ev [29] gave two constructions of perfect codes with the method of concatenation. In 1988 Solov'eva presented another class of perfect codes [22] and generalized it with Vasil'ev in [28]. In 1994 Vardy and Etzion described a class of perfect codes of full rank [8]. There are also three codes of length 15 (Bauer et al. [7]) and three codes of length 15 described by Heden in [10]. In 1995 Phelps and LeVan [17] presented perfect codes with all possible sizes of kernels. In 1996 Avgustinovich and Solov'eva [3] gave a construction of perfect codes which led to a new lower bound

on the number of different perfect codes. In 1996 Lobstein and Zinov'ev generalized the 'concatenation construction' of perfect codes [13].

4. Upper bounds

Knowing the number of all perfect codes of a certain length n it is easy to calculate the number of nonequivalent perfect codes, therefore we will treat equivalent codes as different codes. There is only an upper bound on the number of different perfect codes close to a trivial bound. This bound follows immediately from the following nontrivial properties of perfect codes. Let $\mathbf{1}$ be the all-one vector, i.e. $\mathbf{1}=(1,1,\ldots,1)$.

Property 1 (Shapiro and Slotnik [20]). *For every codeword $\alpha\in C$ we have $\alpha\oplus\mathbf{1}\in C$.*

Property 2 (Shapiro and Slotnik [20]). *The number of codewords of weight $(n-1)/2$ of a perfect code of length n is equal to*

$$M_n=\left(\binom{n}{(n-1)/2}+n(-1)^{(n+1)/4}\binom{(n-1)/2}{(n-3)/4}\right)\Big/(n+1).$$

Property 3 (Avgustinovich [2]). *Every perfect code of length n is uniquely determined by its codewords of weight $(n-1)/2$.*

Denoting by T_n the number of all vectors of weight $(n-1)/2$ of the n-cube E^n, we obtain from these properties the following upper bound on the number N_n of different perfect codes

$$N_n\leqslant\binom{T_n}{M_n}\leqslant 2^{2^{n-(3/2)\log n+\log\log(en)}}.$$

Here and below $\log n$ is always the binary logarithm.

The trivial upper bound is

$$2^{2^{n-\log n+\log\log(n+1)}}.$$

5. Vasil'ev codes, lower bound

Let V^p be a perfect code of length $p=2^k-1$, $k\geqslant 2$. Let λ be an arbitrary function from V^p to the set $\{0,1\}$. For $\gamma\in E^p$ let $|\gamma|=\gamma_1+\cdots+\gamma_p(\mathrm{mod}\,2)$, where $\gamma=(\gamma_1,\ldots,\gamma_p)$. Set $n=2p+1$.

Theorem 1 (Vasil'ev [27]). *The set $V^n=\{(\gamma,\gamma\oplus\beta,\ |\gamma|\oplus\lambda(\beta)):\gamma\in E^p,\beta\in V^p\}$ is a perfect code of length n.*

Since λ is an arbitrary function, we obtain (taking in account the previous iterative steps) the following lower bound on the number of different perfect codes:

$$N(V^n) \geqslant 2^{2^{(n+1)/2} - \log(n+1)} \cdot 2^{2^{(n+5)/4} - \log(n+1)},$$

where $N(V^n)$ denotes the number of Vasil'ev codes of length n.

This bound has been the best lower bound for a long time. The lower bounds given by Phelps [16] and Solov'eva [22] are of the form

$$2^{2^{((n+1)/2)}(1-\varepsilon_n)},$$

where $\varepsilon_n \to 0$ if $n \to \infty$.

Some inessential improvement of $N(V^n)$ can be obtained by Mollard's construction [14]. We now consider his construction.

6. Mollard codes, lower bound

Let C^r and C^m be two perfect codes of length r and m, respectively. Let

$$\alpha = (\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1m}, \alpha_{21}, \ldots, \alpha_{2m}, \ldots, \alpha_{r1}, \ldots, \alpha_{rm}) \in E^{rm}.$$

The generalized parity functions $p_1(\alpha)$ and $p_2(\alpha)$ are defined by $p_1(\alpha) = (\sigma_1, \sigma_2, \ldots, \sigma_r) \in E^r$, $p_2(\alpha) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_m) \in E^m$, where $\sigma_i = \sum_{j=1}^{m} \alpha_{ij}$ and $\sigma'_j = \sum_{i=1}^{r} \alpha_{ij}$. Let f be an arbitrary function from C^r to E^m.

Theorem 2 (Mollard [14]). *The set*

$$M^n = \{(\alpha, \beta \oplus p_1(\alpha), \gamma \oplus p_2(\alpha) \oplus f(\beta)) : \alpha \in E^{rm}, \beta \in C^r, \gamma \in C^m\}$$

is a perfect code of length $n = rm + r + m$.

In the case $m = 1$, Mollard's and Vasil'ev's constructions coincide. Solov'eva [24] has proved the existence of Mollard codes which are not Vasil'ev codes.

7. $\tilde{\alpha}$-components, lower bound

We now develop a lower bound on the number of different perfect codes of length n.

First some definitions. Let C be a perfect code in E^n, $n = 2^k - 1$, $k \geqslant 2$, and let M be a subset of C. Exchanging the bit in the i'th coordinate of all vectors of M with the opposite bit we obtain a new set, denoted by $M \oplus i$. If $C' = (C \setminus M) \cup (M \oplus i)$ is a perfect code, we call the set M an *i-component* of the code C and say that C' is obtained from C by a *translation* of an i-component M.

Let $\tilde{\alpha} \subseteq \{1, \ldots, n\}$. The set M is called an *$\tilde{\alpha}$-component* of the code C if it is an i-component for every $i \in \tilde{\alpha}$.

An i-component is *minimal* if it cannot be subdivided into smaller i-components. The concept of i-components (in the terminology of disjunctive normal forms) was introduced by Vasil'ev [27]. From Vasil'ev's construction it is easy to see that the set $\{(\gamma,\gamma,|\gamma|) : \gamma \in E^p\}$ is always an n-component of V^n, $n = 2p+1$.

It is known [22,23] that upper and lower bounds on the number m of minimal i-components of an arbitrary perfect code of length n, $n = 2^k - 1$, are given by

$$2 \leqslant m \leqslant 2^{(n+1)/2}/(n+1).$$

Both of these bounds can be achieved, see [27,22,23]. The cardinality of the minimal i-components can vary from $2^{(n-1)/2}$ to $2^{n-1}/(n+1)$. Therefore, choosing successively some of n coordinates and exchanging some of the components, we can obtain a great variety of perfect codes. Denote by H^* the set of all perfect codes obtained in this way from the Hamming code. The question of whether every perfect code can be obtained from a Hamming code in such a way was raised in [3]. Phelps and LeVan [19] presented a perfect code of length 15 and showed that it does not belong to H^*.

Now we give the description of the construction of Avgustinovich and Solov'eva [3,6]. Let H^n be the Hamming code of length n (a linear perfect code). Let $\{i,j,k\}$ be the vector of H^n of weight 3 with only the ith, jth and kth coordinates equal to 1 and $N_1 = 2^{(n+5)/4-\log(n+1)}$, $N_2 = 2^{(n-3)/4}$.

Proposition 1. *The Hamming code H^n can be partitioned in $\{i,j,k\}$-components R^t_{ijk}*

$$H^n = \bigcup_{t=1}^{N_1} R^t_{ijk}.$$

Proposition 2. *Every $\{i,j,k\}$-component R^t_{ijk}, $t = 1,\ldots,N_1$, can be partitioned in i-components R^l_i.*

$$R^t_{ijk} = \bigcup_{l=1}^{N_2} R^l_i.$$

We now choose for every $\{i,j,k\}$-component R^t_{ijk} one of the coordinates i,j or k and divide the $\{i,j,k\}$-component into the components in the chosen coordinate. Thus the code H^n is split into the i-, j- and k-components with minimal cardinalities. This partitioning of the Hamming code allows us to construct (cf. [3,6]) a large class of different perfect binary codes.

Theorem 3. *There are at least*

$$2^{2^{(n+1)/2-\log(n+1)}\,6^{2^{(n+5)/4-\log(n+1)}}}$$

different perfect binary codes of length n.

This bound is better than the other known lower bounds.

It is not difficult to see that this construction method is possible for the Hamming code divided into some $\tilde{\alpha}$-components, where every $\tilde{\alpha}$-component is divided into $\tilde{\alpha}'$-components, $\tilde{\alpha}' \subseteq \tilde{\alpha}$. Such partitions yield complicated classes of perfect codes. We restrict ourselves to the case which gave us the maximal factor in the lower bound of Theorem 3.

8. Nonsystematic perfect codes

We now continue to describe some properties of perfect codes.

The technique of $\tilde{\alpha}$-components allowed Avgustinovich and Solov'eva [4,5] to obtain nonsystematic perfect binary codes of length n for every $n = 2^k - 1$, $k \geqslant 8$. The question about the existence of nonsystematic perfect codes was posed by Hergert [11]. A perfect code C of length n is systematic if there are $n - \log(n+1)$ coordinates (called information symbols) such that the code C deleted in the remaining $\log(n+1)$ coordinates (called check symbols) coincides with $E^{n-\log(n+1)}$.

Proposition 3. *Let $n = 2^k - 1$, $k \geqslant 8$. There are n minimal components $M_1, \ldots, M_n$ with minimal cardinalities in the Hamming code H^n such that the i'th component M_i is an i-component and the distance between two components M_i and M_j is more than 5 if $i \neq j$.*

This property allows us to exchange every i-component M_i in the i'th coordinate. With this we obtain

Theorem 4 (Augustinovich and Solov'eva [4,5]). *The set*

$$C = \left(H^n \setminus \left(\bigcup_{i=1}^{n} M_i \right) \right) \cup \left(\bigcup_{i=1}^{n} (M_i \oplus i) \right)$$

is a nonsystematic perfect code of length n for every $n = 2^k - 1$, $k \geqslant 8$.

The existence of nonsystematic perfect codes of length $n = 2^k - 1$, $5 \leqslant k \leqslant 7$, was proved by Phelps and LeVan [18].

9. Isometries of perfect codes

Let φ be an *isometric* map from C to C', i.e. a map between two perfect codes C and C' such that $d(x, y) = d(\varphi(x), \varphi(y))$ for every $x, y \in C$.

Theorem 5 (Avgustinovich [1]). *Let $n > 15$ and C, C' be any two isometric perfect codes. Then they are isomorphic.*

It is also true if $n = 15$ but if $n = 7$ there exists the isometric map φ from H^7 to H^7 such that φ is not extendable to an isomorphism of the whole space E^7, see [25].

10. Kernels of perfect codes

Let $C \subseteq E^n$ be a code. The set K of all vectors $x \in E^n$, for which $C \oplus x = C$ is called the kernel of C.

Heden [10] found three perfect codes of length 15 which have kernels of dimensions 1–3.

Phelps and LeVan [17] established the following result.

Theorem 6. *For all $k \geqslant 4$ there exists a nonlinear perfect code of length $n = 2^k - 1$ which has a kernel of dimension j if and only if $j \in \{1, 2, \ldots, 2^k - k - 3\}$.*

Studying kernels and $\tilde{\alpha}$-components may be helpful for the decision of the complicatedly seeming question if two given perfect codes are equivalent.

Acknowledgements

The author is grateful to Werner Heise and the anonymous referees for comments improving the presentation of the paper.

References

[1] S.V. Avgustinovich, On nonisometry of perfect binary codes, Proc. Inst. Math. SO RAN 27 (1994) 3–5.
[2] S.V. Avgustinovich, On a property of perfect binary codes, Discrete Anal. Oper. Res. 2 (1) (1995) 4–6.
[3] S.V. Avgustinovich, F.I. Solov'eva, Construction of perfect binary codes by sequential translations of the i-components Proceedings of the Fifth International Workshop on Algebraic and Combinational Coding Theory Sozopol, Bulgaria, June 1996, pp. 9–14.
[4] S.V. Avgustinovich, F.I. Solov'eva, Existence of nonsystematic perfect binary codes, Proceedings of the Fifth International Workshop on Algebraic and Combinational Coding Theory, Sozopol, Bulgaria, June 1996, pp. 15–19.
[5] S.V. Avgustinovich, F.I. Solov'eva, On the nonsystematic perfect binary codes, Problems Inform. Transmission 32 (3) (1996) 258–261.
[6] S.V. Avgustinovich, F.I. Solov'eva, Construction of perfect binary codes by sequential translations of an $\tilde{\alpha}$-components, Problemy Peredachi Informatzii 33 (3) (1997) 15–21 (in Russian).
[7] H. Bauer, B. Ganter, F. Hergert, Algebraic techniques for nonlinear codes, Combinatorica 3 (1983) 21–33.
[8] T. Etzion, A. Vardy, Perfect binary codes: Constructions, properties and enumeration, IEEE Trans. Inform. Theory 40 (3) (1994) 754–763.
[9] O. Heden, A new construction of group and nongroup perfect codes, Inform. Control 34 (4) (1977) 314–323.
[10] O. Heden, A binary perfect code of length 15 and codimension 0, Designs Codes Cryptography 4 (1994) 213–220.
[11] F. Hergert, Algebraische Methoden fur Nichtlineare Codes, Thesis, Darmstadt, 1985.

[12] J.-M. Laborde, Une nouvelle famille de codes binaires, parfaits, non linéaires, C.R. Acad. Sci. Paris 297 (1) (1983) 67–70.
[13] A.C. Lobstein, V.A. Zinov'ev, On new perfect binary nonlinear codes, Appl. Algebra Eng. Commun. Comput. 8 (1997) 415–420.
[14] M. Mollard, A generalized parity function and its use in the construction of perfect codes, SIAM J. Algebraic Discrete Methods 7 (1) (1986) 113–115.
[15] K.T. Phelps, A combinatorial construction of perfect codes, SIAM J. Algebraic Discrete Methods 4 (3) (1983) 398–403.
[16] K.T. Phelps, A general product construction for error correcting codes, SIAM J. Algebraic Discrete Methods 5 (2) (1984) 224–229.
[17] K.T. Phelps, M.J. LeVan, Kernels of nonlinear Hamming codes, Designs Codes Cryptography 6 (1995) 247–257.
[18] K.T. Phelps, M.J. LeVan, Non-systematic perfect codes, SIAM J. Discrete Math. 12 (1) (1999) 27–34.
[19] K.T. Phelps, M.J. LeVan, Switching equivalence classes of perfect codes, Designs, Codes and Cryptography 16 (2) (1999) 179–184.
[20] G.S. Shapiro, D.L. Slotnik, On the mathematical theory of error correcting codes, IBM J. Res. Develop. 3 (1) (1959) 25–34.
[21] F.I. Solov'eva, On binary nongroup codes, Methody Discretnogo Analiza 37 (1981) 65–76 (in Russian).
[22] F.I. Solov'eva, Factorization of code-generating disjunctive normal forms, Methody Discretnogo Analiza 47 (1988) 66–88 (in Russian).
[23] F.I. Solov'eva, Exact bounds on the connectivity of code-generating disjunctive normal forms, Inst. Math. Siberian Branch of Acad. Sci. USSR, Preprint 10 (1990) 15 (in Russian).
[24] F.I. Solov'eva, A combinatorial construction of perfect binary codes, Proceedings of the Fourth International Workshop on Algebraic and Combinational Coding Theory, Novgorod, Russia, September, 1994, pp. 171–174.
[25] F.I. Solov'eva, S.V. Avgustinovich, T. Honold, W. Heise, On the extendability of code isometries, J. of Geometry 61 (1998) 3–16.
[26] A. Tietäväinen, On the nonexistence of perfect codes over finite fields, SIAM J. Appl. Math. 24 (1973) 88–96.
[27] Y.L. Vasil'ev, On nongroup close-packed codes, Problems Cybernet. 8 (1962) 375–378 (in Russian).
[28] Y.L. Vasil'ev, F.I. Solov'eva, Interdependence between perfect binary codes and their projections, Proceedings of the Seventh Joint Swedish–Russian Workshop on Information Theory, St. Petersburg, Russia. June, 1995, pp. 239–242.
[29] V.A. Zinov'ev, A combinatorial methods for the construction and analysis of nonlinear error-correcting codes, Ph.D. Thesis, Moscow, 1988 (in Russian).
[30] V.A. Zinov'ev, V.K. Leontiev, A theorem on nonexistence of perfect codes over Galois fields, Inst. Problems Inform. Transmission, Preprint, 1972 (in Russian).
[31] V.A. Zinov'ev, V.K. Leontiev, On perfect codes, Problems Control Inform. Theory 1 (1972) 26–35.
[32] V.A. Zinov'ev, V.K. Leontiev, Nonexistence of perfect codes over Galois fields, Problems Control Inform. Theory 2 (2) (1973) 123–132.